CHAPTER 10

PHYSICAL SECURITY

Physical security is that part of security concerned with physical measures designed to safeguard personnel; to prevent unauthorized access to equipment, facilities, material, computer media, and documents; and to safeguard them against espionage, sabotage, damage, and theft. This chapter addresses the many facets of a physical security program.

PHYSICAL SECURITY DEFINITIONS

LEARNING OBJECTIVE Define 12 terms that apply to physical security programs.

The following definitions apply to the physical security programs as discussed in this chapter:

- *Activity*. Any unit of the Naval Shore Establishment of distinct identity and established under an officer in command or in charge, by direction from appropriate authority.

- *Auxiliary Security Force (ASF).* An armed force composed of local, nondeploying military assets derived from host and tenant commands under the operational control of the host command's security department. The ASF is used to augment the installation's permanent security force during increased threat conditions or when directed by the host command.

- *Counterterrorism.* Offensive measures taken to prevent, deter, and respond to terrorism.

- *Exception.* A written, approved, long-term (36 months or longer) or permanent deviation from a specific security requirement.

- *Facility.* A real property entity consisting of one or more of the following: a building, a structure, a utility system, pavement, and underlying land.

- *Installation.* A grouping of facilities, located in the same vicinity, that support particular functions. Installations may be elements of a base.

- *Pilferage.* Petty larceny; stealing of small items, generally stored goods.

- *Property.* All assets, including real property, facilities, funds, and negotiable instruments; arms, ammunitions, and explosives; tools and equipment; material and supplies; microwave towers; communication antennas and power transformers; computer hardware and software; and information in the form of documents and other media, whether categorized as routine or special, unclassified or classified, nonsensitive or sensitive, conventional or nuclear, critical, valuable or precious.

- *Plan of action and milestones (POA&M).* A written document identifying specific security deficiencies, corrective courses of action, and expected dates of completion.

- *Security manager.* An individual, appointed in writing by the commanding officer, responsible for the development, implementation, and management of the command's Information and Personnel Security Program. The security manager acts as the commanding officer's principal advisor in matters pertaining to the security of classified information.

- *Security officer.* An individual appointed in writing by the commanding officer, who is responsible for the development, implementation, and management of the command's Law Enforcement and Physical Security Program.

- *Waiver.* A written temporary relief, normally for a period of 1 year, from specific security requirements, pending actions or accomplishment of action that will result in conformance with the minimum security standards.

SECURITY RESPONSIBILITIES

LEARNING OBJECTIVES: Explain individual responsibility for security in the Navy. List the specific responsibilities of the commanding officer, security officer, and security manager. Describe the composition of a security department, and list the five basic categories of duties of a security department. Explain the organizational role of the security officer in a command's security program.

Security is the direct responsibility of every person (military and civilian) in the Department of the Navy.

To have a good physical security program, the program must receive command attention and direction from all echelons within the chain of command. The physical security functions should be carried out by well-trained personnel. Much emphasis is placed on the commanding officer to make sure the commands security posture is accurately assessed and that security resources are appropriate to execute these programs.

COMMANDING OFFICER

The commanding officer of an activity is ultimately responsible for all security, including physical security, within that activity. The commanding officer makes the appointment of an adequately trained and/or experienced security officer to develop and manage the physical security program, which is paramount to the command's mission. The commanding officer also provides sufficient resources, staff assistance, and authority to the security officer to implement, manage, and execute an effective Physical Security and Loss Prevention Program.

SECURITY OFFICER

The security officer is designated in writing by the commanding officer. The security officer reports directly to the commanding officer, keeping the executive officer informed, and is responsible in assisting the commanding officer by determining the adequacy of the command's Physical Security and Loss Prevention Program. The security officer identifies those areas where improved physical security and loss prevention are required. Chapter 1 of the *Physical Security and Loss Prevention Manual,* OPNAVINST 5530.14, covers in detail how the security officer performs his or her duties.

The level of training/experience required of the Physical Security Officer varies, depending upon the complexity, size, and mission of the activity. In smaller commands, the security officer position may be a collateral duty requiring only limited security training or experience and may be, in commands of less than 200 personnel, assigned to a senior enlisted (E-7 or above) with appropriate experience or training. In larger commands, installations, and bases, the security officer billet is assigned to a fully trained or experienced commissioned officer or warrant officer and is normally treated as a department head tour.

SECURITY MANAGER

The security manager is the commanding officer's advisor and direct representative in matters pertaining to the security of classified material. In the performance of these duties, the security manager is guided by OPNAVINST 5510.1. The security officer supports the security manager in protecting classified material. The security manager may serve concurrently as the security officer.

SECURITY DEPARTMENT

The security department is comprised of personnel specifically trained, organized, and equipped to provide the security required to protect an activity's assets and is the single most important element of a command's security program.

Security departments may be composed of military, civilian, or contract guards, or any combination thereof. Regardless of the type or composition of the security department, the duties will fall into five basic categories:

1. Protection of life, property, and the rights of individual citizens

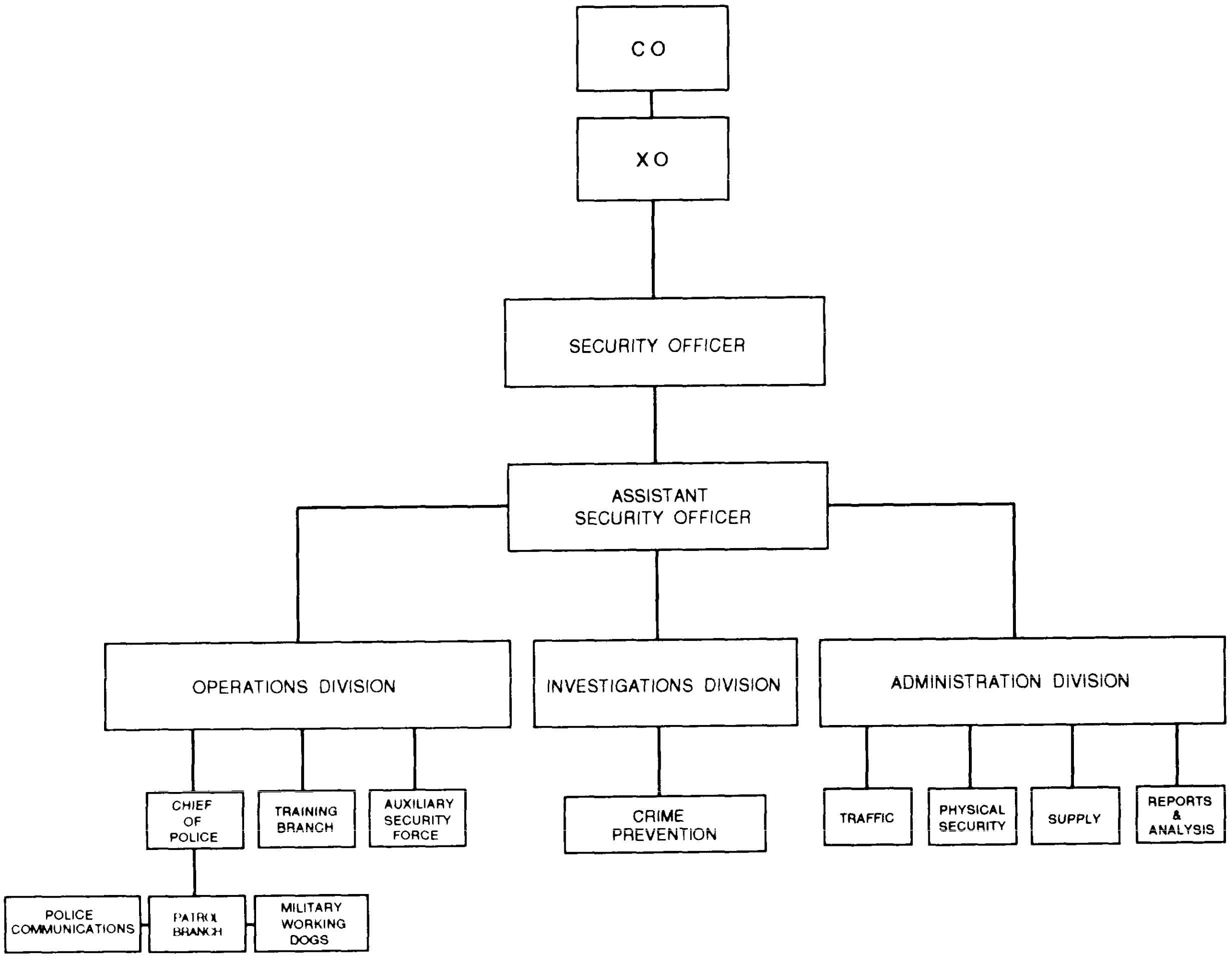
2. Enforcement of Federal/local laws, ordinances, rules and regulations

3. Preserving the peace; preventing, detecting, and investigating accidents and crimes; arresting violators; and aiding citizens in emergency situations

4. Preventing or deterring theft, other losses, fire, damage, accidents, trespassing, sabotage or espionage

5. Controlling pedestrian and vehicular traffic

Commands where the security department has both a law enforcement and physical security mission (normally the host activity) should be organized as shown in figure 10-1. The Operations Division is responsible for all security and law enforcement functions, such as patrol, traffic, harbor security, Auxiliary Security Force, and training. The Administration Division is responsible for all administrative functions associated with the Security Department including, but not limited to, physical security, loss prevention, and access control. The Investigations Division is primarily responsible for the investigation of all cases not under the jurisdiction of the Naval Criminal Investigative Service (NCIS) and will maintain a close liaison with the local supporting NCIS Office.



1 ASSISTANT SECURITY OFFICER POSITION IS NOT REQUIRED
2 A COMMAND MAY IDENTIFY ADDITIONAL DIVISIONS AS REQUIRED BY MISSION
3 A COMMAND MAY IDENTIFY ADDITIONAL BRANCHES AS REQUIRED BY MISSION

Figure 10-1.-Security department.

Deputy security officers should be assigned to supervise each of the three major branches—a Deputy Security Officer for Operations (formally Chief of Police); Deputy Security Officer for Administration; and the Deputy Security Officer for Investigations (formally Chief Investigator). Each of the deputies should report directly to the Security Officer.

ORGANIZATIONAL RELATIONSHIPS

The security officer serves, via the executive officer, as the commanding officer's principal advisor in all matters relating to physical security. Close coordination between the security officer and personnel assigned to other security disciplines, such as the security manager, the automated information security (AIS) officer, and the operations security (OPSEC) officer, is essential for the success of a viable program. In smaller activities, it is not uncommon for the security officer to serve as the security manager or the manager of other specialized security programs. Additionally, the security officer may work directly for the security manager or vice versa, depending upon the nature of the command's mission and/or the predominate type of property held by the command.

SECURITY COMMITTEES

LEARNING OBJECTIVES: Describe the three required forums for day-to-day management of security programs.

Coordination is an important building block in any security program and is essential in its day-to-day management. In this section, we discuss three of the required and most widely used forums.

PHYSICAL SECURITY REVIEW COMMITTEE

Every naval activity, regardless of size or mission, is required to establish a Physical Security Review Committee (PSRC) to review and discuss security matters as they pertain to that particular command. The PSRC is appointed in writing by the commanding officer or officer in charge and should be chaired by the activity security officer. Membership in the PSRC is normally comprised of the following command personnel:

- Security officer (chairperson).
- Commanding Officer, Marine Corps Security Barracks/Company or, as appropriate, the senior member of the activity Marine Corps cadre.
- Comptroller.
- Security manager and officers or managers of other specialized security programs (for example, base/activity police/guard supervisor, ADP security officer).
- Public works officer or facilities manager.
- Supply officer.
- Legal officer or general counsel.
- Directors/heads of activities/installations and major command functions whose missions are influenced and impacted by security requirements.
- Senior rated Master-at-Arms, or senior designated Master-at-Arms, assigned physical security duties.
- Internal review functional manager.
- Weapons/ordnance officer.
- Naval Criminal Investigative Service. A representative of the NCIS, while not listed in the required membership, should be included.

LOSS PREVENTION SUBCOMMITTEE

In addition to the PSRC, all naval activities are required to establish a Loss Prevention Subcommittee (LPS), which normally meets immediately following the PSRC meeting. Membership within the LPS should consist of at least three PSRC members, including internal review participation. The purpose of the LPS is to conduct loss trends analysis, review and tabulate losses, determine preventive and disciplinary measures to be taken, and track actions pending. Minutes for the LPS may be appended to those of the PSRC. In commands of less than 200 assigned personnel, the LPS may meet semi annually versus quarterly. As an alternative, membership in the host command's LPS may meet the LPS requirement.

PHYSICAL SECURITY REVIEW BOARD

The physical security review board (PSRB) is very similar in composition and mission to that of the PSRC. It is, however, designed to address security-related matters on a base or installation-wide perspective. The PSRB is chaired by the host command/activity, and its membership is comprised of representatives of all tenant command/activities. The primary goal of the PSRB is the coordination of mutually supportive physical security and loss prevention practices. Minutes from PSRB meetings should be made a matter of record and retained by the host command in the same manner prescribed for PSRC minutes.

COMMAND KEY CONTROL

LEARNING OBJECTIVES: Describe the criteria for selection and the duties of the key control officer, key custodian, and key subcustodian. Explain the purpose of the key control room and the importance of a well-organized key center. Explain the use of lock control seals and the procedure for lockouts.

Command key control is a vital part of a command's physical security program. In this section, we discuss the responsibilities of key control personnel and key control procedures.

KEY CONTROL OFFICER

A command key control officer should be designated in writing by the commanding officer. Personnel selected should have a Secret security clearance, or more ideally, a security clearance equal to the highest level of classified material held at the command. Selecting personnel with a proven ability to organize is also helpful. Smaller commands may find it best to select the security officer/manager as the key control officer because of the close ties to the facility's emergency services and control. The person selected should have a good working relationstip with the security department.

KEY CUSTODIAN

A key custodian should be designated in writing by the key control officer. The person selected should hold a security clearance at least equal to the assets controlled by the key and lock program. Personnel from within the security department are excellent choices because of the focus on working relationships with the security department. In smaller commands, the key custodian and key control officer may be the same person.

KEY SUBCUSTODIANS

Key subcustodians should be designated by their respective department heads or tenant commands and approved in writing by the key control officer. These personnel may be given control of one or more sub master keys, depending upon the need and mission. For example, the fire department may be designated as a key subcustodian and may have access to all facility keys. Departments may be subcustodians, but the mission of one may require a different key application than that of another. Reliability and integrity play very important roles in the selection of a key subcustodian. The security clearance of subcustodians should be equal to the highest classified level of material secured.

CENTRAL KEY ROOM

Duplicate keys, key blanks, padlocks, and key-making equipment should be secured in a central key room according to OPNAVINST 5530.14. Access should be limited to the commanding officer, key control officer, key custodian, and locksmith. This room should have restricted access and be secured when not in use. Key blanks and duplicate keys should be given the same classification protection as the original keys. At commands too small to warrant or require a central key room, a GSA-approved security container with a three-position combination lock may be used to protect duplicate keys, blanks, and associated equipment as described in OPNAVINST 5530.14. Key codes should also be kept in the central key room. These codes should be kept in an authorized security container as previously discussed.

KEY CENTERS

The importance of an effective index-coordinated key center cannot be overstated. These centers should be co-located with 24-hour staffed sites, such as emergency services dispatch centers. Adequate personnel should also be considered when evaluating a key issue point so that any diversions to the issuer's attention will not compromise the program's integrity. Ingress and egress to and from the key issue point should not compromise the dispatcher or operator in any way. Smaller commands located independently from a major facility may not have a 24-hour emergency support center. The key control should be handled by the key control officer or custodian as required by the commanding officer and according to with Navy policy.

LOCK CONTROL SEALS

Inactive or infrequently used gates must be locked and have seals affixed. The approved seal is a car ball end seal, Military Specification MIL-S-23769C. Security personnel should be instructed that lack of free play (approximately one-eighth inch) indicates the possibility of tampering and a follow-up examination of the seal should be conducted. All seals should be serialized and stored in the same manner as keys. All unused seals should be inventoried annually. The security officer should control placement of entrance seals and account for seals on hand, issued, and used.

LOCKOUTS

Lockouts occur when a lock becomes inoperable for some reason; all lockouts involving restricted areas or buildings should be investigated by security personnel. The investigation should determine if the failure occurred because of lock malfunction or as a result of attempted or actual unlawful entry.

SECURITY INSPECTIONS

LEARNING OBJECTIVES: Explain the importance of security inspections and the reporting requirements for security inspections. Describe quarterdeck inspections, administrative inspection of vehicles, and the exemption for NCIS personnel.

Each naval activity must establish a system for the daily after hours checking of restricted areas, facilities, containers, and barrier or building ingress and egress points to detect any deficiencies or violations of security standards. Security deficiencies or violations found during after hour checks should be reported to the activity security officer, the department involved and the commanding officer. These incidents should also be reported to activity departments or other local elements having security responsibilities within specific security programs affected by the incident. Each deficiency or violation should be followed up by the activity security officer, and a record kept of all actions taken (structural, security, disciplinary, administrative, and so on) by the responsible department or other organizational elements involved to resolve the present deficiency or violation and to prevent recurrence. All security deficiencies, violations, breaches of security rules and regulations, and criminal incidents discovered and handled by the security force will be recorded on OPNAV Form 5527/1.

QUARTERDECK INSPECTIONS

Quarterdeck inspections should be conducted according to OPNAVINST 3120.32. No person should refuse to present for inspection by the OOD/authorized personnel or Master-at-Arms any item of baggage or article in his or her possession or on his or her person or knowingly conceal in any container or on his or her person any article with intent to deceive or evade the lawful inspection of such articles.

ADMINISTRATIVE INSPECTION OF VEHICLES

All vehicles on naval installations are subject to administrative inspection according to procedures authorized by the commanding officer. As ordered and directed by the commanding officer, authorized security personnel will, while in the performance of assigned duties, administratively inspect vehicles entering or leaving the installation. Such inspections are deemed reasonably necessary to protect the premises, material, and utilities from loss, damage, or destruction.

Because important constitutional questions are involved, no person or group maybe exempted from, or singled out for, such inspections. And the instruction by commanding officers regarding such inspections should be coordinated in advance of implementation with the local JAG or Naval Legal Service Office officials to ensure strict adherence to a structured random inspection pattern.

At the minimum, guards should be instructed that incoming persons and automobiles may not be inspected over the objection of the individual. However, those who refuse to permit inspection should not be allowed to enter. Persons who enter should be advised in advance (a properly worded sign to this effect prominently displayed in front of the access point will suffice) that they and their vehicles are subject to inspection while on board the installation and upon departure. Persons who refuse to submit their vehicle to an authorized inspection while on board or upon departure may be detained long enough to obtain a warrant for search of the vehicle, issuance of a letter barring future entrance to the installation, or such other action as may be appropriate.

EXEMPTION FOR NAVAL CRIMINAL INVESTIGATIVE SERVICE

NCIS personnel and their vehicles, used in the course of official business, are exempt from administrative inspection of vehicles upon presentation of a badge and/or credentials when entering or leaving Navy installations.

PERIMETER AND AREA PROTECTION AND CONTROL

LEARNING OBJECTIVES: Explain the reason for conducting a risk and threat analysis. Explain the concept of enclaving. Describe the two types of area designations.

Before a decision to use security measures is made, a thorough risk and threat analysis should be performed to determine the degree of physical security required. As reflected in paragraph 0203 of OPNAVINST 5530.14: “In certain cases, extensive and costly security measures may be necessary to protect certain items of security interest. However, in each case the commanding officer of an activity is responsible for complying with established security requirements while at the same time working to achieve economy. To achieve this objective, higher echelon security requirements must be clearly understood. Additionally, the relative criticality and vulnerability of the security interest must be evaluated in relation to a ranking of potential threats, and a specific level of security must be calculated to ensure the best possible protection for that threat level in a cost-effective manner.” Only after these preliminary factors are addressed can proper controls be instituted.

Installation or perimeter and area protective controls are the first steps in providing actual protection against certain security hazards. These controls are obtained through the use of protective barriers and other security measures. They are intended to define the installation/activity/area boundaries and are used to channel personnel and vehicular access. Security barriers may be natural or structural and are addressed in chapter 6 of OPNAVINST 5530.14.

ENCLAVING (ISLAND) SECURITY CONCEPT

Enclaving is the preferred method for securing relatively small restricted areas at specific sites within an installation. These areas include naval readiness or other critical assets requiring a higher degree of protection than the installation itself. Enclaving involves segregating certain areas and concentrating security resources for these areas, which is generally more cost-effective than fencing the entire perimeter. For instance, a restricted area may be enclaved by a separate fence, lighting, or alarm system, without fencing the entire installation perimeter.

As in the case for the protection of arms, ammunition, and explosives according to OPNAVINST 5530.13, installing standard chain link fencing around the entire outer perimeter of certain naval installations may not be consistent with attempts by the Federal government to retrocede legislative jurisdiction to state authorities for certain areas aboard naval installations. Examples include Navy and Marine Corps exchanges and financial, recreational, and medical facilities.

Enclaving does not eliminate the requirement to identify and post installation perimeters. This could be accomplished by installing alternate fencing, such as two- to four-strand barbed wire.

Installations that elect to adopt enclaving to protect assets as a temporary or permanent alternative to required perimeter standard fencing must submit a waiver or exception request per paragraph 0116 of OPNAVINST 5530.14. Requests must indicate the type of perimeter fencing planned and/or other compensatory security measures planned or in place.

AREA DESIGNATIONS

Different areas and tasks require different degrees of security interest depending upon their purposes, nature of the work performed within, and the information and/or materials concerned. For similar reasons, different areas within an activity may have varying degrees of security importance. To address these situations, facilitate operations and simplify the security system. A careful application of restrictions, controls, and protective measures commensurate with varying degrees or levels of security importance is essential. In some cases, the entire area of an activity may have a uniform degree of security importance requiring only one level of restriction and control. In others, differences in the degree of security importance will require further segregation of certain security interests.

Areas will be designated as either restricted areas or nonrestricted areas. Restricted areas are established in writing by a commanding officer within his or her jurisdiction. These areas are established "pursuant to lawful authority and promulgated pursuant to DOD Directive 5200.8, dated 29 July 1980 (enclosed in SECNAVINST 5511.36), and Section 21, Internal Security Act of 1950; Ch. 1024, 64 stat. 1005; 50 U.S.C. 797)."

Now let's look at restricted and nonrestricted areas in more detail.

RESTRICTED AND NONRESTRICTED AREAS

LEARNING OBJECTIVES: Identify and explain the three types of restricted areas. Define a *nonrestricted area.*

Three types of restricted areas are established in descending order of importance–Level Three. Level Two, and-Level One. All restricted areas should be posted simply as Restricted Areas (according to sign provisions set forth in the following paragraphs) so as not to single out or draw attention to the importance or criticality of an area. While restricted areas often pertain to the safeguarding of classified information, there are other valid reasons to establish restricted areas, such as mission sensitivity; protection of certain unclassified chemicals; precious metals or precious-metal-bearing articles; conventional arms, ammunition and explosives; finds; drugs; nuclear material; sensitive or critical assets; or articles having high likelihood of theft.

LEVEL THREE (FORMERLY EXCLUSION AREA)

Level Three is the most secure type of restricted area It may be within less secure types of restricted areas. It contains a security interest that, if lost, stolen, compromised or sabotaged, would cause *grave damage* to the command mission or national security. Access to the Level Three restricted area constitutes, or is considered to constitute, actual access to the security interest or asset.

LEVEL TWO (FORMERLY LIMITED AREA)

The second most secure type of restricted area is Level Two. It may be inside a Level One area, but is never inside a Level Three area. It contains a security interest that, if lost, stolen, compromised, or sabotaged, would cause *serious damage* to the command mission or national security. Uncontrolled or unescorted movement could permit access to the security interest.

LEVEL ONE (FORMERLY CONTROLLED AREA)

Level One is the least secure type of restricted area. It contains a security interest that, if lost, stolen, compromised, or sabotaged, would cause *damage* to the command mission or national security. It may also serve as a buffer zone for Level Three and Level Two restricted areas, thus providing administrative control, safety, and protection against sabotage, disruption, or potentially threatening acts. Uncontrolled movement may or may not permit access to a security interest or asset.

NONRESTRICTED AREAS

A nonrestricted area is an area, under the jurisdiction of an activity, where access is either minimally controlled or uncontrolled. Such an area may be fenced or open to uncontrolled movement of the general public. An example of a nonrestricted area is a visitor or employee parking lot that is open and unattended by guards. After business hours it may be closed patrolled, and converted to a restricted area. Another example is a personnel office where the general public is permitted access during business hours without being required to check in or register with the security office. A nonrestricted area maybe an area enclosed by a fence or other barrier, where access is minimally controlled by a checkpoint only, ensuring that the visit or access was for an authorized purpose. In such cases, further security authorization (a security clearance) would not be required for access. A housing area exterior to the base would normally be designated as a nonrestricted area. Nonrestricted areas should not be located inside restricted areas.

Many activities and installations have areas containing a number of facilities where members of the Armed Forces and their dependents, as well as civilian employees and their families, are permitted access by displaying vehicle decals or by presenting appropriate identification cards (not issued on the basis of security clearance or similar screening, but by virtue of employment or status). These facilities include exchanges, commissaries, administrative offices, dispensaries, clubs, recreational facilities, and so on. Areas containing these facilities on activities and installations will normally be designated as nonrestricted areas. However, these facilities themselves may have internal spaces that will, of necessity, be designated as restricted areas.

MINIMUM SECURITY MEASURES

LEARNING OBJECTIVES: List and explain the minimum security measures for each type of restricted area. Explain the general security measures taken within restricted areas.

Each type of restricted area requires a certain minimum level of protection. Except as indicated in OPNAVINST 5530.14, classification of each type of restricted area is the responsibility of the commanding officer. Now let's consider the minimum security measures required for each level.

LEVEL THREE SECURITY MEASURES

The following minimum security measures are required for Level Three restricted areas:

- A clearly defined protected perimeter. The perimeter may be a fence, the exterior walls of a building or structure, or the outside walls of a space within a building or structure. If the perimeter is a fence, it should be posted at no less than 100-foot intervals along the perimeter. Barrier and lighting requirements are set forth in chapters 6 and 7 of OPNAVINST 5530.14. If the perimeter is a wall, it should be posted at the point of ingress.

- A personnel identification and control system, including an access list and entry and departure log. Only visitors need be logged in and out during normal duty hours. After normal duty hours, all personnel should be logged in and out.

- Ingress and egress controlled by guards or appropriately trained and cleared personnel. When secured, access to the area should be controlled by an intrusion detection system or security personnel.

- Admission only to persons whose duties require access and who have been granted appropriate authorization. Persons who have not been cleared for access to the security interest contained within a Level Three restricted area may, with appropriate approval, be admitted to such area, but they should be controlled by a cleared activity or facility escort at all times and the security interest protected from compromise.

- When secured, the area should be checked at least twice per 8-hour shift, or at least once per 8-hour shift if adequately equipped with an operational intrusion system. The security force should check for signs of attempted or successful unauthorized entry and for other activity that could degrade the security of the Level Three restricted area.

LEVEL TWO SECURITY MEASURES

The following minimum security measures are required for Level Two restricted areas:

- A clearly defined and protected perimeter. The perimeter may be a fence, the exterior walls of a building/ structure or the outside walls of a space within a building/structure. If the perimeter is a fence, it should be posted at no less than 100-foot intervals along the perimeter. If the perimeter is a wall, it should be posted at the point of ingress.

- A personnel identification and control system. During normal duty hours, use of an access list and entry and departure log is suggested but not required. After normal duty hours, all personnel should be logged in and out. (An electronic control system with the capability of recording ingress and egress may be used to accomplish this.) If a computer access control or logging system is used, it should be safeguarded against tampering.

- Both ingress and egress should be controlled by guards, receptionists, or other appropriately trained and cleared personnel and secured during nonworking hours.

- Admission should be granted only to persons whose duties require access and who have been granted appropriate authorization. Persons not cleared for access to the security interest contained within a Level Two restricted area may, with appropriate approval, be admitted, but they should be controlled by a cleared activity escort at all times, and the security interest protected from compromise.

- When secured, the area should be checked at least twice per 8-hour shift or at least once per 8-hour shift if adequately equipped with an operational intrusion system. The security force should check for signs of attempted or successful unauthorized entry and for other activity that could degrade the security of the Level Two restricted area.

LEVEL ONE SECURITY MEASURES

The following minimum security measures are required for Level One restricted areas:

- A clearly defined protected perimeter. The perimeter may be a fence, exterior walls, or outside walls of a space within a building or structure. If the perimeter is a fence, it should be posted at no less than 100-foot intervals along the perimeter. If the perimeter is a wall, it should be posted at the point of ingress.

- A personnel identification and control system.

- Ingress and egress controlled by guards, receptionists, or other appropriately trained and cleared personnel.

- Controlled admission of individuals (military, civil service, contractors, official visitors) who require access for reasons of employment or official business, individuals who render a service (vendors, delivery people), dependents, retired military, and unofficial visitors (guests of residents, visiting softball team). Individuals without adequate identification, as determined by the local commanding officer, should be logged in and out.

GENERAL SECURITY MEASURES

Certain facilities and assets identified as critical and essential to the overall mission of the Navy and Marine Corps and national security have been identified in appendix IX of OPNAVINST 5530.14. Restricted area designations have been assigned in addition to specific physical security requirements to provide optimum protection.

All instructions designating restricted areas should include procedures for conducting inspections of persons and vehicles entering and leaving such areas. The purpose is to detect and prevent the introduction of prohibited items (firearms, explosives, and drugs) and to detect and prevent the unauthorized removal of government property and material. To be effective, administrative vehicle and personnel inspection operations should be conducted daily on a random basis. As a minimum, the activity's security officer should make sure they are conducted at least weekly.

Procedures should be coordinated with the cognizant Staff Judge Advocate or Naval Legal Service Office and approved by the activity commanding officer or designated representative.

LIMITED WATERWAY AREAS

LEARNING OBJECTIVES: List and define four types of limited waterway areas. Determine the agency responsible for each area and list the authority, limitations, penalties, enforcement, and threat required.

Installation/activity commanding officers should ensure their waterfront and waterway areas are designated by proper authority. Commanding officers of installations/activities adjacent to waterways having, or seeking to establish, control mechanisms to limit persons, vehicles, vessels and objects within designated areas have several options. This section describes the different types of limited waterway areas available based on the level of threat. The U.S. Coast Guard (USCG) and U.S. Army Corps of Engineers (USACE) may, when safety, security, or other national interests dictate, control access to and movement within certain areas under their jurisdiction.

Table 10-1 describes the area, agency, authority, limitations, penalties, and enforcement of the four types of limited waterway areas. The Comments section of table 10-1 provides information regarding threat justification. For more information on limited waterway areas, see OPNAVINST 5530.14.

Commanding officers should make every effort to coordinate protection of adjacent waterway areas with the proper agency, and they should also review operations and security plans to make sure areas of responsibility are properly identified. Liaison between security personnel and local Coast Guard officials should be maintained to ensure designation of limited waterway areas and that procedural aspects are kept current.

SIGNS AND POSTING OF BOUNDARIES

LEARNING OBJECTIVES: Determine the size, color and posting points for ingress and perimeter barrier signs for both restricted and nonrestricted areas.

Restricted areas, including buildings, should be posted at regularly used external points of ingress with signs approximately 3 feet by 3 feet, with proportionate lettering. Signs should read as follows:

WARNING

RESTRICTED AREA - KEEP OUT

AUTHORIZED PERSONNEL ONLY

AUTHORIZED ENTRY INTO THIS RESTRICTED AREA CONSTITUTES CONSENT TO SEARCH OF PERSONNEL AND THE PROPERTY UNDER THEIR CONTROL.

INTERNAL SECURITY ACT OF 1950 SECTION 21; 50 U.S.C. 797

Criteria for identifying internal points of ingress into designated restricted and nonrestricted buildings are contained in OPNAVINST 5510.1.

Perimeter barriers of all restricted areas should be posted with signs measuring approximately 12 inches by 18 inches, with proportionate lettering. Signs should read as follows:

WARNING

RESTRICTED AREA

KEEP OUT

Authorized Personnel Only

Nonrestricted areas should be posted at all points of ingress with signs approximately 3 feet by 3 feet, with proportionate lettering. Signs should read as follows:

WARNING

U.S. NAVY PROPERTY

AUTHORIZED PERSONNEL ONLY

AUTHORIZED ENTRY ONTO THIS INSTALLATION CONSTITUTES CONSENT TO SEARCH OF PERSONNEL AND THE PROPERTY UNDER THEIR CONTROL.

INTERNAL SECURITY ACT OF 1950 SECTION 21; 50 U.S.C. 797

Perimeters of nonrestricted areas should be posted with signs measuring approximatel 11 inches by 12 inches, with proportionate lettering. Signs should read as follows:

U.S. GOVERNMENT PROPERTY

NO TRESPASSING

Table 10-14-Limited Waterway Areas

LIMITED WATERWAY AREAS						
AREA	AGENCY	AUTHORITY	LIMITATIONS	PENALTIES	ENFORCEMENT	COMMENTS
*RESTRICTED AREA	USACE(1)	33 CFR 207	Only on inland waters.	Misdemeanor	Enforcement can be delegated to the Navy command.	No threat needed. Easy to obtain. Provides limited area jurisdiction for command.
*SAFETY ZONE	USCG/ COTP(2)	33 CFR 165	Temporary, but may be long term	Misdemeanor Can result in civil or criminal penalties under 33 USC 1232.	USCG only. Navy may patrol. COTP authority.	No threat needed. Can be placed around "moving" vessel.
*SECURITY ZONE	USCG/ COTP	Magnuson Act (50 USC 191)/ 33 CFR 6.10-5, 33 CFR 165	Only within territorial limits of United States. No person or vessel may enter zone without permission from COTP. Can be placed overland.	Felony - 10 years/$10,000	USCG only. Navy may patrol under COTP authority.	Threat required. COTP controls access and movement of all vessels, persons & vehicles (including their removal), and may take possession and control of any vessel. (See 33 CFR 165.33.)
*RESTRICTED WATERFRONT AREAS	USCG/ COMDT (3)	Magnuson Act (50 USC 191) 33 CFR 165.40	Must be issued and directed by Commandant of the Coast Guard. COTP may be directed to enforce. Must be in regulations. Limits access of persons.	Felony - 10 years/$10,000	USCG only. COTP directed by COMDT.	Threat required. Long-term limited access area. Any change must be directed by the COMDT.
(1) USACE - U.S. Army Corps of Engineers (2) COTP - Coast Guard Captain of the Port (3) COMDT - Commandant of the Coast Guard * Does not include airspace						

Where a language other than English is prevalent, restricted and nonrestricted area warning notices should be posted in both languages.

The interval between signs posted along restricted and nonrestricted area perimeters should not exceed 200 feet. All barrier signs should be placed so as not to obscure the necessary lines of vision for security force personnel.

All signs should be color-coded to provide legibility from a distance of at least 100 feet during daylight under normal conditions. The following color codes are recommended for installation/activity and restricted/nonrestricted area perimeter signs:

- All words except *WARNING* should be black.
- The word *WARNING* should be red.
- All wording should be on red, white, and/or blue backgrounds, as appropriate, to obtain maximum color contrast.

Warning signs not worded as prescribed in the previous paragraphs should be replaced. Waivers/exceptions are not required.

PROTECTIVE LIGHTING

LEARNING OBJECTIVES: Explain the purpose and value of protective lighting. Identify nine basic principles of protective lighting. Evaluate three types of protective lighting systems. Explain the power requirements for emergency lighting systems.

Protective lighting provides a means of continuing a degree of security approaching that which is maintained during daylight hours. It increases the effectiveness of security forces performing their duties, has considerable value as a deterrent to thieves and vandals, and may make the job of the saboteur or terrorist more difficult. Requirements for protective lighting at an activity depend upon the situation and the areas to be protected. In the interest of finding the best possible mix between energy conservation and effective security, each situation must be carefully studied. The overall goal is to provide the proper environment to perform duties such as identification of badges and personnel at gates and inspection of unusual or suspicious circumstances. Where lighting is impractical, additional compensating measures should be instituted.

GENERAL PRINCIPLES AND GUIDELINES

NAVFAC MIL-HDBK-1013/1 provides general principles and guidelines for exterior protective lighting. These guidelines, including table 25 and table 26 of this reference, should be applied by activities when determining protective lighting requirements. When protective lighting is installed and used, the previous guidelines and the following basic principles should be applied:

- Provide adequate illumination or compensating measures to discourage or detect attempts to enter restricted areas and to reveal the presence of unauthorized persons within such areas.
- Avoid glare that handicaps security force personnel or is objectionable to air, rail, highway or navigable water traffic or occupants of adjacent properties.
- Locate light sources so that illumination is directed toward likely avenues of approach and provides relative darkness for patrol roads, paths, and posts. To minimize exposure of security force personnel, lighting at entry points should be directed at the gate and the guard should be in the shadows. This type of lighting technique is often called *glare projection.*
- Illuminate shadowed areas caused by structures within or adjacent to restricted areas.
- Design the system to provide overlapping light distribution. Equipment selection should be designed to resist the effects of environmental conditions, and all components of the system should be located to provide maximum protection against intentional damage.
- Meet requirements of blackout and coastal dimout areas.
- Avoid drawing unwanted attention to restricted areas.
- During planning stages, consideration should be given to future requirements of closed circuit television (CCTV) and recognition factors involved in selection of the type of lighting to be installed. Where color recognition will be a factor, full spectrum (such as high-pressure sodium vapor) lighting vice single color should be used.
- Choose lights that illuminate the ground or water but not the air above. These lights must penetrate fog and rain.

TYPES OF PROTECTIVE LIGHTING SYSTEMS

There are several types of protective lighting systems in use today. Each should receive consideration by the command based on their requirements. We will touch on three of these systems: continuous, standby, and movable. We will also discuss some emergency power requirements.

Continuous Lighting

The most common protective lighting system is a series of fixed lights arranged to flood a given area continuously with overlapping cones of light. The two primary methods of employing continuous lighting are glare projection and controlled lighting.

GLARE PROJECTION LIGHTING.– Glare projection lighting uses lights slightly inside a security perimeter and directed outward. This method is useful where the glare of lights directed across surrounding territory will neither annoy nor interfere with adjacent operations. It is a deterrent to potential intruders because it makes it difficult to see inside the area being protected. It also protects security personnel by keeping them in comparative darkness and enabling them to observe intruders at a considerable distance beyond the perimeter.

CONTROLLED LIGHTING.– Controlled lighting is best used when it is necessary to limit the width of the lighted strip outside the perimeter because of adjoining property or nearby highways, railways, navigable water, or airports. The width of the lighted strip can be controlled and adjusted to fit a particular need, such as illumination of a wide strip inside a fence. Care should be taken to minimize or eliminate silhouetting or illuminating security personnel on patrol.

Standby Lighting

A standby system differs from continuous lighting insofar as its intent is to create an impression of activity. The lights are not continuously lighted, but are either automatically or manually turned on randomly or when suspicious activity is detected or suspected by security personnel or intrusion system. Lamps with short restart times are essential if this technique is chosen. This technique may offer significant deterrent value while also offering economy in power consumption.

Movable Lighting

Movable lighting (stationary or portable) consists of manually operated searchlights that may be lighted during hours of darkness or as needed. ‘This system is normally used to supplement continuous or standby lighting.

EMERGENCY LIGHTING

Emergency lighting may duplicate any or all of the previous systems. Its use is limited to times of power failure or other emergencies that render the normal system inoperative. It depends on alternative power sources, such as installed or portable generators or batteries.

PROTECTIVE LIGHTING PARAMETERS

LEARNING OBJECTIVES: List five criteria that commanding officers should use to determine protective lighting requirements. Explain the minimum standards for protective lighting and the need for an emergency power source. Identify the technical aspects and describe switch and control protection for protective lighting systems.

The commanding officer must decide what other areas or assets to illuminate and how to do it. This decision should be based upon the following criteria:

- Relative value of items being protected
- Significance of the items being protected in relation to the activity mission and its role in the overall national defense structure
- Availability of security forces to patrol and observe illuminated areas
- Availability of fiscal resources (procurement, installation, and maintenance costs)
- Energy conservation

MINIMUM STANDARDS

Unpatrollable fence lines, water boundaries, and similar areas need not be illuminated. Where these areas are patrolled, sufficient illumination should be provided to assist the security force in preventing intrusion.

Vehicular and pedestrian gates used for routine ingress and egress should be sufficiently illuminated to facilitate personnel identification and access control.

Exterior building doors should be provided with lighting to enable the security force to observe an intruder seeking access.

Airfields, aircraft, shipyards, controlled industrial areas, piers, docks, petroleum storage areas, and other mission-critical areas should be protected with sufficient illumination for the security force to detect, observe, and apprehend intruders.

Protective lighting should be checked daily by the security force to ensure all light fixtures are operational. Inoperative lights should be recorded and referred to the security officer.

The security officer should make sure all reports of inoperative protective lights are given immediate attention and corrective actions are taken.

EMERGENCY POWER

Restricted areas provided with protective lighting should have an emergency power source located within the restricted area. The emergency power source should be adequate to sustain security lighting and communications requirements and other essential services required within restricted areas. Provisions should be made to ensure the immediate availability of the emergency power in the event of failure of the primary source. Emergency power sources should start automatically. Battery-powered lights and essential communications should be available at all times at key locations within the restricted areas in the event of complete failure of primary and emergency sources of power. Emergency power systems should be tested monthly and the results should be recorded/logged and maintained for a period of 3 years or until the next cognizant Inspector General command inspection cycle, whichever is greater.

TECHNICAL ASPECTS

The differences in building arrangements, terrain, atmospheric conditions, and other factors necessitate the designing of each protective lighting system to meet the conditions peculiar to each activity or facility.

Protective illumination should not be curtailed below the minimum required for security. Lack of illumination contributes to increases in loss and vandalism that can more than offset energy costs. In designing a lighting system, consideration should be given to local conditions at the installation or activity, with efforts concentrated on reducing the amount of energy used to deliver the illumination required by taking advantage of all lighting energy conservation opportunities (LECO). LECO should be evaluated in terms of existing systems in the area and future requirements.

A lighting energy audit should be conducted to learn what is installed, the condition, the energy being consumed, the light produced, the amount of light needed, and so forth, to determine which type of lamp (incandescent, fluorescent, mercury vapor, metal halide, high-pressure sodium, or low-pressure sodium) system or systems would be best.

New system interactions should be evaluated with existing systems in adjacent areas to determine impact (other light levels, electrical transmission systems, heating and cooling systems, and so on).

Multiple circuits may be used to an advantage in protective lighting systems. The circuits should be so arranged that the failure of anyone lamp will not darken a long section of a critical or vulnerable area. The protective lighting system should be independent of other lighting systems and should be protected so that a fire or disaster will not interrupt the entire system.

SWITCH AND CONTROL PROTECTION

Controls and switches for protective lighting systems should be inside the protected area and locked or guarded at all times. An alternative is to locate the controls in a central station similar to, or as a part of, the system used in intrusion detection alarm central monitoring stations. High-impact plastic shields may be installed over lights to prevent destruction by stones, air rifles, and so on.

PHYSICAL SECURITY SURVEYS

LEARNING OBJECTIVES: List and explain the purpose of a physical security survey. Describe the three types of physical security surveys.

Each Navy activity and installation should establish a program to assess the degree of local compliance with the security standards, requirements, and policies on an annual basis. The physical security survey checklist contained in appendix VIII of OPNAVINST 5530.14 should be used. Command inspections or special-purpose (physical security inspection/physical security audit/physical security review) examinations of an activity's security program should be conducted by an immediate superior in command at least every 3 years. This survey should include the practical exercise of physical security, loss prevention, and crisis management plans to evaluate the overall adequacy of the security force. It should also evaluate the activity's ability to protect against penetration of its barriers and unauthorized entry, protect vital property, and deal with terrorist situations.

PURPOSE OF PHYSICAL SECURITY SURVEYS

Physical security surveys are used to evaluate the adequacy of a command's security program. The security officer should initiate physical security surveys, which may be conducted by rated Master-at-Arms, trained civilian employees, or security guard force personnel. Physical security surveys should be conducted at least once annually. These surveys should identify all security discrepancies and make recommendations for corrective actions. Additionally, a POA&M should be developed to assist in the tracking of corrective actions taken and pending.

A physical security survey is made to verify current information and to obtain new facts. It should be conducted not only during normal duty hours but also during nonduty hours, including hours of darkness. If done correctly, the survey will provide a true picture of the existing hazards and effectiveness of current protective measures. Physical security surveys should be used as a management tool and are not normally sent up the chain of command.

TYPES OF PHYSICAL SECURITY SURVEYS

Three types of physical security surveys are used on installations: initial, supplemental, and follow-up. Each is discussed in turn.

Initial Survey

The *initial* survey is the very first survey of an installation and is conducted by the responsible surveying office.

Supplemental Survey

A *supplemental* survey is conducted when changes occur in the organization, mission, or physical aspects that would affect physical security of the installation.

Follow-up Survey

The *follow-up* survey is made to ensure recommendations from the initial and supplement surveys have been carried out. It is important to make sure work orders are initiated and stay valid.

CONTROL OF PERSONNEL

LEARNING OBJECTIVES: Describe seven types of personnel identification systems and the characteristics of each. Explain standard re-badging and badge expiration dates. Explain expiration dates for permanent picture, military permanent, and contractor picture badges. Describe 6 standards and 10 characteristics of passes and badges. Explain key card control.

The reason for establishing a personnel control system is to provide a visible means to track and identify personnel who are authorized access to certain areas and to deny access to those who are not authorized. The degree of control should be in keeping with the sensitivity, classification, or operational importance of the area. It is important to keep the procedures simple. Visitor control should be in compliance with OPNAVINST 5510.1.

PERSONNEL IDENTIFICATION SYSTEMS

The following types of personnel identification systems may be used independently or in conjunction with each other:

- Military/Dependent Identification Cards. May be used as a medium to identify personnel authorized access to areas that do not have security implications (nonrestricted areas). This system is considered the least reliable means for determining access authorization.

- U.S. Government Identification Card. Civil service employees may be issued U.S. Government Identification Cards, Optional Form 55, to identify civilian employees and may be used as a means to authorize access into areas that do not have security implications.

- Personal Recognition: The most positive method of identification and should be used in areas where the number of authorized personnel does not exceed 50.

- Access List System. Admission of individuals to restricted areas should be granted to only those persons who are positively identified. To assist in their identification process, access lists may be used to control access into Level 1 and Level 2 areas, and are required in all Level 3 areas. Access lists should be maintained and kept under stringent control of an individual who is formally designated by the commanding officer. Lists must be protected from public view and, if a computerized system is used, it should be safeguarded against tampering.

- Pass and Badge System. For access to large areas or where the number of personnel exceeds that allowed for personal recognition, a pass and badge system should be used. This system is considered the most practical means of identification to be used by large activities. Minimum badging standards and criteria are contained in chapter 5 of OPNAVINST 5530.14.

- Exchange Pass System. The exchange pass system is employed in highly sensitive areas (Levels One and Two restricted areas). It involves exchanging one or more identification media (badges, passes, and so on) for another type of identifier.

- Escort System. Escorting is a method of identifying and controlling personnel within a security area who are not normally authorized access to that area. The assigned escort should remain with the visitor at all times while he or she is within the security area.

STANDARD RE-BADGING

Installations and activities should re-badge all regular employees and other personnel possessing permanent picture badges every 6 years or when a loss of 6 percent is attained, whichever occurs first.

A loss of 6 percent is the maximum acceptable standard for the reissue of permanent picture identification badges. To compute the percentage of lost permanent badges, divide the number of lost permanent badges by the number of permanent badges issued over a given period of time, normally from the beginning of the current 6-year time period. Losses totaling 6 percent or more require re-badging.

New permanent picture badges should be distinctly different from those replaced.

BADGE EXPIRATION DATES

All issued security badges and passes should bear an expiration date. The expiration date should be conspicuously displayed on the face of the badge or pass and should be distinguishable from a distance of 3 feet during normal daylight hours. Now let's look at expiration dates for permanent picture, military permanent, and contractor picture badges.

Permanent Picture Badges

All permanent picture badges issued during a 6-year period to nonmilitary personnel should bear the same expiration date. For example, badges issued during a 6-year period ending in December 1993 would normally bear a December 1993 expiration date. If unscheduled re-badging is required during any 6-year cycle, a new 6-year cycle would start from the date of the unscheduled re-badging and expiration would be 6 years from that date.

Military Permanent Badges

All permanent picture badges issued to military personnel stationed on an activity should expire at the end of their projected rotation date (PRD), expiration of TAD, TEMDUINS or TDY, or expiration of active obligated service (EAOS), whichever occurs first.

Contractor Picture Badges

Contractor picture badges should expire at the completion of the current contract or 24 months, whichever occurs first.

PASS AND BADGE STANDARDS

The following guidelines apply when a pass or badge system of identification is necessary:

- An activity's permanent ID pass or badge must contain all of the characteristics listed below and set forth in OPNAVINST 5530.14.

- A temporary pass or badge need not contain all of the characteristics listed below, since it only provides control of visitors and personnel who visit infrequently. However, the badges should be rigidly controlled and accounted for by individual serial number, should be distinctly different in style and design from permanent passes or badges used by an activity, and should clearly indicate the period and limits of authorized use.

- Pass and badge format may be designed locally. Economy should be considered. The design agency should bear in mind that the primary purpose of an identification system is to control access to specific areas and alert personnel of the presence of unauthorized persons in the area. Bold print; large, recent photographs; a distinctive design; and tamper-resistant structures are prime considerations.

- The "exchange badge system" should be employed where security requirements dictate.

- The printer's plates for passes or badges should be obtained and safeguarded to avoid compromise. When necessary, the pass system may be changed by reprinting in different colors or reformatting the pass.

- The badge or pass form should be serialized controlled, and protected. The issuing activity should conduct an inventory of all serially numbered badges and passes on hand at least semiannually and should establish written procedures for retrieval and destruction of invalid badges and passes from personnel whose access has been terminated.

PASS AND BADGE CHARACTERISTICS

The following characteristics apply to permanent passes or badges:

- Size, which is generally consistent with other standard identification cards.

- A photograph; minimum size is 1 inch by 1 1/4 inch (same as military ID card). The maximum size should be consistent with economy, available equipment, and pass or badge design. The photograph should be in color, stress facial features, and should not include the area below the neck.

- A clear space at the top of the pass or badge to place a hole for an attachment device.

- A serial number for accountability.

- Name of holder, typewritten or printed.

- Signature of holder.

- Name, rank, and title of validating officer.

- Signature of validating officer.

- Expiration date of pass/badge.

- The following statements are required and may be incorporated in the badge design or be an overlay on the lamination. They may be combined:

"U.S. Government Property."
"Loss of this card must be reported at once"
"If found, drop in nearest U.S. mailbox."

"Postmaster: Postage Guaranteed. Return to Commanding Officer, (address of the issuing activity indicated on face of badge)."

"Warning - issued for official use of the holder designated hereon. Use or possession by any other person is unlawful and will make the offender liable to penalty - 18 U.S.C. 499, 506, 701." (Reference should be made to the Status of Forces Agreements for overseas activities only.)

Security construction requirements should include heat seal adhesion of the complete card to prevent photographic reproduction. An identifying logo or validation seal or initials should be manufactured into the lamination along with other positive security measures that will help prevent tampering. Identifying information should be clearly legible to security personnel at a distance of 1 meter in normal lighting conditions.

KEY CARDS

Where card readers are used to control access, procedures for removal or invalidation of lost key cards from the system and changes to personnel identification numbers for associated digital key pads should be included.

CONTROL OF VEHICLES

LEARNING OBJECTIVES: Explain how the vehicle decal is used to control privately owned vehicles and how decals are used in overseas areas. Describe how passes are used for visitor control. Explain why vehicle passes issued by other activities are honored. Describe the special precautions that should be considered in vehicle control.

Directly related to the movement and access control of personnel is the control of various privately owned motor vehicles. The standard Navy Decal, DD Form 2220, is the media used to identify and control motor vehicles on most installations. Whatever media is used, it should serve as a rapid means of identifying the vehicle as having authority for being operated and parked on the installation. It should not be used as a mean to identify the driver or any occupant.

APPLICATION OF DECALS IN OVERSEAS AREAS

Certain overseas activities and other locations where terrorist activity is acute and ongoing may be exempt from the provisions of this requirement and OPNAVINST 5560.10 and OPNAVINST 11200.5. Stronger emphasis should be placed on positive identification and control of vehicles and occupants entering installations and activities exempt from the requirement to display vehicle decals. At small activities, the use of vehicle access lists could be employed to provide positive vehicle identification. The use of portable decals displayed on the windshield of vehicles is discouraged because of potential theft and illegal use of these decals. Personal recognition continues to be the best method of identification and should be used whenever possible. Those activities meeting this criteria and desiring to be exempt must obtain an exception to the requirement, according to paragraph 0116 in OPNAVINST 5530.14.

VISITOR CONTROL

Vehicles requiring only temporary access may be issued locally produced temporary vehicle passes. A large card displayed on the sun visor or windshield may be used as a temporary pass.

A temporary pass may be printed in several colors that can be changed periodically to detect unauthorized use. In addition to identification information, the following warning should be included:

> **Acceptance of this pass constitutes your consent to inspection of this vehicle and occupants therein by security force personnel when entering, aboard, or leaving this station. Visitors aboard this installation are guests of the commanding officer and, as such, should conduct themselves in accordance with the limited conditions under which the invitation is extended. Political activities, pamphleteering, speeches, demonstrations, placard/banner displays, or other similar conduct will not be permitted without prior written permission of the commanding officer. Persons violating these conditions will have their invitations withdrawn, be removed from the installation, and are subject to prosecution.**

Commercial vehicles may be authorized entry by permanent registration or visitor control methods. In addition to the normal administrative inspection procedures, additional precautions should be taken to prevent the introduction or removal of unauthorized material or personnel.

HONORING OF VEHICLE IDENTIFICATION

Since military, retired military personnel, and certain civil service employees will generally have personal or official requirements to enter nearby military activities in their private automobiles, the honoring of DOD vehicle identification media issued by other activities is allowed, according to OPNAVINST 5560.10.

SPECIAL PRECAUTIONS

Personnel responsible for the accomplishment or implementation of personnel and vehicle control procedures should at all times be watchful for the unauthorized introduction to or removal from the installation of government property, especially weapons, ammunition, and explosive materials. This surveillance should encompass all personnel and means of transportation, including government, private, and commercial vehicles, aircraft, railcars, and ships.

INTRUSION DETECTION SYSTEMS

LEARNING OBJECTIVES: State the purpose of Intrusion Detection Systems (IDSs). Identify 6 advantages of IDSs and list 10 factors to consider when these systems are employed. Describe four types of IDSs.

Intrusion Detection Systems (IDSs) are an essential element of any in-depth physical security program. IDSs consist of sensors capable of detecting one or more types of phenomena, signal media, annunciators, and energy sources for signaling the entry or attempted entry into the area protected by the system. The design, implementation, and operation of the IDS should contribute to the overall physical security posture and the attainment of security objectives. IDSs are designed to detect, not prevent, actual or attempted penetrations. Therefore, IDSs are useless unless supported by near-real-time assessment systems and prompt security force response when the systems are activated.

The advantages of IDSs include the following:

- Permit more economical and efficient use of security personnel through the employment of mobile responding security forces instead of fixed guard posts and/or patrols

- Provide additional controls at critical areas or points

- Substitute for other physical security measures that cannot be used because of safety regulations, operational requirements, building layout, cost, or similar reasons

- Provide insurance against human error

- Enhance the security force capability to detect and defeat intruders

- Provide the earliest practical warning to security forces of any attempted penetration of protected areas

IDS EMPLOYMENT FACTORS

The following factors should be considered in determining the feasibility and necessity of installing IDS equipment:

- Mission
- Criticality
- Threat
- Geographic location of the installation or facility and location of facilities to be protected within each activity or installation
- Accessibility to intruders
- Availability of other forms of protection
- Life cycle cost of the system
- Construction of the building or facility
- Hours of operation
- Availability of a security force and expected response time to an alarm condition

TYPES OF INTRUSION DETECTION SYSTEMS

There are basically four types of IDSs: the local alarm; central station; police connection; and proprietary. Each of these systems will be discussed in turn.

Local Alarm

In the local alarm system, the protective circuits and alarm devices actuate a visible or audible signal in the immediate vicinity, usually on the exterior of the building. The alarm transmission/communication lines do not leave the building. Response is by local security forces that may be in the area when the alarm is sounded. Otherwise, the security force will only know of the alarm if it is reported by a passerby or found during routine checks. The disadvantage of this system is that intruders know exactly when the alarm is activated and can easily elude capture. This system should be used only when guards can respond in a timely manner.

Central Station

In the central station system, the operation of alarm devices and electrical circuits are automatically signaled to, recorded in, maintained and supervised from a central station owned and managed by a commercial firm with guards and operators in attendance at all times. These personnel monitor the signals and provide the response force to any unauthorized entry into the protected area. Connection of alarm equipment to the central station is usually over leased telephone company lines. The provisions of paragraph 0809c in OPNAVINST 5530.14 apply.

Police Connection

In the police connection system, the alarm devices and electrical circuits are connected via leased telephone company lines to a monitoring unit located in nearby civilian police stations. An agreement with the local police department must be arranged before establishment of this type of system. The provisions of paragraph 0809c in OPNAVINST 5530.14 apply.

Proprietary

The proprietary IDS is the prescribed IDS for all naval activities and installations. This system is quite similar to a central station operation except that the IDS monitoring/recording equipment for all IDSs at the installation is located within a constantly manned security force communications center maintained and owned by the government installation. The installation security force responds to all IDS activations. Connection of the alarm sensor equipment to the security force central monitoring station is normally over leased telephone company lines or by separate cable owned and installed by the installation. If a computerized IDS is used, it must be safeguarded against tampering.

IDS EQUIPMENT DESCRIPTION

LEARNING OBJECTIVES: Explain exterior and interior sensors. Describe the following subsystems: data transmission and annunciator, control, and display. Explain the operating power requirements for IDSs.

Each intrusion detection system is comprised of various types of equipment that operate in unison to complete the overall detection function. In addition to sensing devices installed at protected locations, data generated by the sensors should be transmitted by electrical impulse to control annunciator display equipment in a central alarm annunciating station. Electrical power should be supplied to all items including backup power. Each equipment category comprises a subsystem and is described in the following paragraphs.

SENSOR SUBSYSTEM

The sensor subsystem is divided into two areas, depending upon environmental use and application: exterior and interior.

Exterior Sensors

Exterior intrusion detection devices (sensors) should be selected for the best performance under prevailing local environmental conditions such as soil, topography, weather, and other factors that could adversely affect performance or increase false alarm (an alarm without a known cause) rates. Exterior IDSs should bean approved DOD standardized system, such as the Base Installation Security System (BISS), or commercial equipment approved by CNO (N09N)/CMC (POS-40), as appropriate, as an element of the DOD standardized system. Presently installed IDSs not meeting the standards of this instruction may continue to be used until replacement is necessary. Waivers or exceptions to use presently installed IDSs are not required.

Interior Sensors

Interior IDSs should be an approved DOD standardized system such as the Joint-Service Interior Intrusion Detection System (J-SIIDS), the AN/GSS-20, or commercial equipment approved by CNO (N09N)/CMC (POS-40), as appropriate, as an element of the DOD standardized system. Presently installed IDSs not meeting the standards of this instruction may continue to be used until replacement is necessary. Waivers or exceptions to use presently installed IDSs are not required

DATA TRANSMISSION SUBSYSTEM

The data transmission subsystem links sensors with control and monitoring consoles. The transmission medium is used to send control signals and data to and from all sensors, control points and annunciator panels. It may be hardwired land lines, radio frequency links, fiber optic cables, or a combination. This vital subsystem is the weakest and most vulnerable of the IDSs and requires protection.

ANNUNCIATOR, CONTROL, AND DISPLAY SUBSYSTEM

The annunciator, control, and display subsystem provides equipment for central operational control and monitoring of the IDSs. Through this equipment, security force personnel are instantly alerted to the status of any protected area. This subsystem should be located in a restricted area and closed off from public view. Alarmed spaces should be designated by zones.

OPERATING POWER REQUIREMENTS

The power to operate an IDS is usually 115-volt ac electrical power, available in each protected area and the security force headquarters except where safety requirements prohibit its use (hazardous storage areas, and so on).

The importance of ensuring that the IDSs will operate continuously cannot be overstated. Each IDS should have an emergency power source to ensure the system's continuous operation. Emergency backup power sources usually consist of rechargeable batteries, or an emergency generator, or both. Paragraph 0809i in OPNAVINST 5530.14 contains a detailed discussion on emergency power sources.

IDS POLICY

LEARNING OBJECTIVES: Explain IDS equipment procurement policy. Describe military construction (MILCON) and OPNAV/CMC designated sites. Explain the policy regarding emergency power, contractor qualifications, installation, and maintenance.

Only IDS standard equipment with formally evaluated capabilities should be used. No IDS should be procured that cannot be supported for the life-span of the equipment, usually 10 years. System design should consider the delay time of associated barriers, location of reaction forces, and the threat to the protected asset. Now let's consider MILCON IDSs AND IDSs for OPNAV/CMC sites.

MILCON IDSs

Facility IDSs that are installed under the MILCON program should be acquired by competitive procurement. Design guidance should be according to NAVFAC DM 13-02 for background and review and NAVFAC NFGS 16727 to match the requirements of the asset to be protected.

IDS FOR OPNAV/CMC-DESIGNATED SITES

Due to the size and complexity of an IDS, certain sites have been designated as OPNAV/CMC. These sites commonly involve both interior and exterior sensors subsystems, electro-46

optical alarm assessment subsystems for perimeter sensors, extensive data transmission networks, and central computers for security monitoring and control. Examples of these types of sites are those storing nuclear weapons, sensitive conventional ordnance, and critical readiness assets. Within the Marine Corps, IDS is centrally managed by CMC (POS-43).

Technical support for system integration, design, procurement, and installation is provided for both services by the Naval Electronics Systems Engineering Center (NAVELEXCEN), Charleston, South Carolina. Naval Electronics Systems Engineering Activity, St. Inigoes, Maryland, provides technical support for closed circuit television subsystems, thermal imagers, and other assessment devices.

Proprietary Type of IDS

All systems within the Navy and Marine Corps should be of the Proprietary type except when used in civilian communities or Reserve Centers. In these circumstances where there is no government force available, the system may be the Police Connection type or Central Station type. Telephone answering services should not be used. If the police connection type is used, formal arrangement should be made with the local police to ensure they monitor and respond to the system.

Emergency Power

An emergency backup (secondary) power source should be provided for operation of the IDSs. This secondary power source should be provided by an uninterrupted emergency generator, if available, or by batteries. Batteries should have adequate capacity to maintain proper operation of the system under normal operating conditions for a minimum of 4 consecutive hours in the event of ac power failure. To calculate the size of batteries, 105 percent of the capacity necessary should be provided and it should be assumed that during the period of operation on backup power, 5 percent of the detection circuits will be in the alarm mode. If a computerized IDS is used, the computer must be provided with a continuous-type uninterruptible power supply (UPS).

Contractor Qualifications

The contractor used to install, service, and/or maintain intrusion detection equipment and/or security alarm systems should be listed by Underwriters Laboratories (UL) in a commercial burglar alarm category for the appropriate level of protection required by the facility and should be staffed and equipped to provide maintenance on the system on a 24-hour-per-day, 7-day-per-week basis with a response time of not more than 4 hours.

The UL requirement for contractors is listed in NAVFAC NFGS-16727. Verification of UL listings can be made by calling the Group Leader of the Burglary Protection and Signaling Department Certification Service. Phone numbers can be obtained from LEPS Teams located in Norfolk, Virginia, or San Diego, California.

INSTALLATION

The following installation procedures should be adhered to:

1. The preferred installation method for all UL-listed IDSs is through qualified personnel from the base public works office or a designated Navy field activity, such as NAVELEXCEN Charleston.

2. Knowledge of the details of a specific IDS may afford an individual the means to effectively bypass the installation. Usually the original installation of an IDS is accomplished under a construction contract, and various elements are involved-the contract document, specifications, detailed drawings, and the actual physical labor necessary to install the device. Sensitive documents, such as the as-built drawings that show both specific design details and locations of components, should be considered for a security classification assigned by the command. Since most IDSs in current use are available on the open market, classification of the systems themselves is not appropriate. The general location of the system is not classified, although its presence should not be publicized. The contract document itself may reveal only sensor locations and

administrative specifications involved in the contract. However, to make sure an IDS is used to protect classified material, contractors should be chosen from those with a facility clearance and only cleared personnel used to install, inspect and maintain IDSs where access to classified interests is involved.

All as-built drawings and a sufficient quantity of maintenance, operator instructions, and engineering and schematic drawings should be provided to the security officer before installation, testing/acceptance.

MAINTENANCE

Proper maintenance of an IDS is imperative. Systems not properly maintained may fail to detect intrusion or yield a high number of false/nuisance alarms, thereby losing credibility and demoralizing the security force to the point where alarm activations may be often ignored. As a result, the level of security may be less than that obtained without an IDS. The more complex an IDS, the more highly skilled and trained the maintenance technicians must be. The number of technicians required to maintain an IDS depends upon the system's complexity and reliability. Vacations, sick leave, coverage of more than one malfunction at a time, and similar factors must also be considered. Maintenance can be provided by trained government personnel (military or civilian) or by contract. The contracting activity should develop procedures to ensure only cleared personnel inspect and maintain an IDS, when considered appropriate by the user activity.

IDS Testing Frequency

All IDSs will be tested at least monthly to make sure the systems are functional. In the conduct of these tests, all individual sensors should be tested to determine the continued adequacy of their intended application. All transmission devices should be validated to ensure proper operations. Testing should be conducted in concert with the security officer. Tests should include the temporary interruption of ac power to make sure ac/dc transfer can be made and batteries or other alternate power sources are functional. Test result records should be retained for 3 years or until the next Inspector General command inspection cycle, whichever is greater.

For perimeter (exterior) IDSs, randomly selected sections (zones) should be tested daily by causing an actual alarm. Depending on the type of sensor, such alarm activations could include touching the fence, walking/running over "protected" ground, or passing through a sensor beam. The sections to be tested should be selected in such a manner that the entire perimeter IDS is tested at least monthly.

Scheduled preventive maintenance should be performed quarterly or more frequently if or when recommended by the equipment manufacturer.

Training

Maintenance training on Navy IDSs installed under OPNAV (N09N) programs is available at Service Schools Command, Great Lakes, Illinois.

Maintenance problems that result in an ineffective IDS are frequently caused by one or more of the following:

- Maintenance personnel not adequately trained or equipped (test equipment, tools, publications)
- System maintenance not assigned a sufficiently high priority
- Insufficient number of maintenance technicians
- Failure to perform routine preventive maintenance
- Lack of proper instructions and/or written procedures for security personnel responsible for operating and monitoring the system
- Failure to maintain a record on system tests, maintenance, false alarms, and similar elements for review of performance trends and potential problems

Supply Support

The availability of replacement parts will also directly affect the maintenance of IDSs. Navy IDSs (in contrast to commercial IDSs) will have supply support in place, commonly at the Ships Parts Control Center (SPCC), Mechanicsburg, Pennsylvania. Specific details on Navy IDS items and their support activity are contained in the Operational Logistic Support Summary (OLSS) given to each completed site.

Detailed information on commercial IDSs component selection and application; sensor/equipment descriptions and layouts; systems design; and installation, maintenance, and testing is contained in NAVFAC DM-13.02. General physical security equipment information is also described in the Naval Civil Engineering Laboratory (L56), Port Hueneme, California publication titled *Physical Security*

Equipment Manual. Information on the Navy IDS program and equipment can be obtained from NAVELEXCEN, Charleston, South Carolina. Information on the Marine Corps IDS program can be obtained from CMC (POS-40).

SUMMARY

In this chapter, we defined several physical security terms and outlined the composition of a security department. Security committees and command key control procedures were also covered. Next, we looked at security inspections and perimeter and area protection and control. We also examined restricted and nonrestricted areas and the minimum security measures required for each area. Limited waterway areas were considered next, and we then looked at signs and posting of boundaries. Protective lighting was also covered, followed by physical security surveys and control of personnel and vehicles. Finally, we examined the types and characteristics of Intrusion Detection Systems (IDSs).